Exponential Separation Between Res(k) and Res($k+1$) for $k \leq \epsilon \log n$

Nathan Segerlind [1]

School of Mathematics
Institute for Advanced Study
Princeton, NJ 08540 USA
nsegerli@math.ias.edu

Abstract

Res(k) is a propositional proof system that extends resolution by working with k-DNFs instead of clauses. We show that there exist constants $\beta, \gamma > 0$ so that if k is a function from positive integers to positive integers so that for all n, $k(n) \leq \beta \log n$, then for each n, there exists a set of clauses $\mathcal{C}_n$ of size $n^{O(1)}$ that has Res($k(n)+1$) refutations of size $n^{O(1)}$, yet every Res($k(n)$) refutation of $\mathcal{C}_n$ has size at least 2^{n^γ}.

Key words: propositional proof complexity, lower bounds, k-DNFs, resolution, res(k), switching lemmas, random restrictions

1 Introduction

Resolution is a propositional proof system that is the foundation of many satisfiability and automated theorem proving algorithms. From the perspective of propositional proof complexity, it is one of the best understood propositional proof systems, with many known size-lower bounds for resolution proofs of well-known tautologies. A resolution proof shows that a formula is a tautology by showing that its negation is unsatisfiable, and this is done by successively deriving clauses using the resolution rule until the empty clause (false) is obtained. The Res(k) systems are generalizations of resolution that are allowed to form k-DNFs as well as clauses. In the same way that resolution proofs correspond to backtracking algorithms for satisfiability that branch upon a single variable, Res(k) proofs correspond to backtracking algorithms that branch upon multiple variables. Moreover, the Res(k) systems can be

[1] Supported by NSF grant DMS-0303258.

viewed as providing intermediate systems between resolution and constant-depth Frege systems.

A natural question to ask is whether or not increasing k, the size of the conjunctions, affects the power of the the proof system Res(k). In this note, we show that there is a constant $\beta > 0$ so that for $k \leq \beta \log n$, Res($k+1$) is exponentially more powerful than Res(k). That is, there exists a family of unsatisfiable sets of clauses $\mathcal{C}_n$ so that for each n, $\mathcal{C}_n$ has Res($k+1$) refutations of size $n^{O(1)}$ yet every Res(k) refutation of $\mathcal{C}_n$ has size at least $2^{n^{\Omega(1)}}$.

The first result separating Res($k+1$) from Res(k) was a separation of Res(2) from Res(1) by Atserias and Bonet using the machinery of monotone interpolation [1]. This result was generalized to a separation between Res($k+1$) and Res(k) for each constant k in [2] (although the same technique works for $k \sim \sqrt{\log n}$). The separation in [2] is shown by use of a *small-restriction switching lemma*. It is a "small-restriction" switching lemma because the random restriction is allowed to set as few as $n^{1-\epsilon}$ out of n variables (contrast with th switching lemma of [3] which must set $n - n^{\epsilon}$ variables). The trade-off is that the switching lemma of [2] converts an OR of very small ANDs into an AND of modestly small ORs. Here, "a very small AND" is one that contains at most $\epsilon\sqrt{\log n}$ variables, where ϵ is a positive constant.

Recently, Alexander Razborov showed that in certain cases the small-restriction switching lemma works for k-DNFs where k is as large as $\epsilon \log n$ (where ϵ is a positive constant) [4]. This works when the k-DNF has a fractional cover by sub-DNFs so that with respect to each sub-DNF the random restriction behaves like a restriction that sets the variables independently *on that sub-DNF*. In this note, we show that the sets of clauses and random restrictions used for the separation for constant k in [2] satisfy the conditions of the newer switching lemma, thereby showing that there is a constant $\beta > 0$ so that Res($k+1$) exponentially dominates Res(k) for $k \leq \beta \log n$.

2 The Resolution and Res(k) Refutation Systems

A resolution refutation of a set of clauses $\mathcal{C}$ is sequences of clauses C_i, $1 \leq i \leq m$, so that C_m is the empty clause, and each C_i either belongs to $\mathcal{C}$ or is inferred by two preceding clauses using the resolution inference: $\frac{A \vee x \quad \neg x \vee B}{A \vee B}$ where $C_j = A \vee x$, $C_k = B \vee \neg x$, $C_i = A \vee B$ and $j, k < i$. Notice that every line in a resolution refutation is a clause. The width of a clause is the number of variables appearing in the clause; the width of a resolution refutation is the width of its widest line. Let $w_R(\mathcal{C})$ denote the minimum width of a resolution refutation of $\mathcal{C}$.

The Res(k) refutation system is a generalization of resolution that can reason using k-DNFs.

Definition 2.1 *Res(k) is the refutation system whose lines are k-DNFs and whose inference rules are given below (A, B are k-DNF's, $1 \leq j \leq k$, and $l, l_1, \ldots, l_j$ are literals):*

$$\textit{Subsumption:} \quad \frac{A}{A \vee l} \qquad\qquad \textit{Cut:} \quad \frac{A \vee \bigwedge_{i=1}^{j} l_i \quad B \vee \bigvee_{i=1}^{j} \neg l_i}{A \vee B}$$

$$\textit{AND-elimination:} \quad \frac{A \vee \bigwedge_{i=1}^{j} l_i}{A \vee l_i} \qquad \textit{AND-introduction:} \quad \frac{A \vee l_1 \ \cdots \ A \vee l_j}{A \vee \bigwedge_{i=1}^{j} l_i}$$

Let $\mathcal{C}$ be a set of k-DNFs. A Res(k) derivation from $\mathcal{C}$ *is a sequence of k-DNFs $F_1, \ldots, F_m$ so that each F_i either belongs to $\mathcal{C}$ or follows from the preceding lines by an application of one of the inference rules. For a set of k-DNFs $\mathcal{C}$, a* Res(k) refutation of $\mathcal{C}$ *is a derivation from $\mathcal{C}$ whose final line is the empty clause. The size of a Res(k) refutation is the number of lines it contains.*

We do not use the exact definition of the *Res(k)* system in our arguments. The only property that we use is the following theorem from [2] that relates the maximum height of the decision trees needed to represent the k-DNFs of a Res(k) derivation to the maximum width of the clauses in the translation of the Res(k) refutation into a resolution refutation.

Definition 2.2 *A* decision tree *is a rooted binary tree in which every internal node is labeled with a variable, the edges leaving a node correspond to whether the variable is set to 0 or 1, and the leaves are labeled with either 0 or 1. Every path from the root to a leaf may be viewed as a partial assignment. For a decision tree T and $v \in \{0,1\}$, we write the set of paths (partial assignments) that lead from the root to a leaf labeled v as $Br_v(T)$. For a partial assignment ρ, $T \restriction_\rho$ is the decision tree obtained by deleting from T every edge whose label conflicts with ρ and contracting along each edge whose label belongs to ρ. We say that a decision tree T* strongly represents *a DNF F if for every $\pi \in Br_0(T)$, for all $t \in F$, $t \restriction_\pi = 0$ and for every $\pi \in Br_1(T)$, there exists $t \in F$, $t \restriction_\pi = 1$. The representation height of F, $H(F)$, is the minimum height of a decision tree strongly representing F.*

Theorem 1 *[2] Let $\mathcal{C}$ be a set of clauses of width $\leq h$. If $\mathcal{C}$ has a Res(k) refutation so that for each line F of the refutation, $h(F) \leq h$, then $w_R(\mathcal{C}) \leq kh$.*

3 The k-Parity Graph Ordering Principles

The unsatisfiable clauses used to obtain the separation are a variation of the graph ordering tautologies [5,6].

Definition 3.1 *Let G be an undirected graph. For each vertex u of G, let $N(u)$ denote the set of neighbors of u in G. For each ordered pair of vertices $(u, v) \in V(G)^2$, with $u \neq v$, let there be a propositional variable $X_{u,v}$.*

The graph ordering principle for G, $GOP(G)$, *is the following set of clauses: (1) The relation X is transitive: for all $u, v, w \in V(G)$, $X_{u,v} \wedge X_{v,w} \rightarrow X_{u,w}$ (2) The relation X is anti-symmetric: for all $u, v \in V(G)$ with $u \neq v$, $\neg X_{u,v} \vee \neg X_{v,u}$ (3) There is no locally X-minimal element: for every $u \in V(G)$, $\bigvee_{v \in N(u)} X_{v,u}$.*

Definition 3.2 *Let $X_1, \ldots, X_k$ be propositional variables. The formula $Odd(X_1, \ldots, X_k)$ is the k-DNF expressing that the number of satisfied variables of $X_1, \ldots, X_k$ is odd. The formula $Even(X_1, \ldots, X_k)$ is the k-DNF expressing that the number of satisfied variables of $X_1, \ldots, X_k$ is even. The* k-parity graph ordering principle of G, $GOP^{\oplus k}(G)$, *is obtained by replacing each literal $X_{u,v}$ by $Odd(X^1_{u,v}, \ldots, X^k_{u,v})$, replacing each literal $\neg X_{u,v}$ by $Even(X^1_{u,v}, \ldots, X^k_{u,v})$, and then using the distributive rule to express this set of k-DNFs as a set of clauses.*

Because every clause of $GOP(G)$ contains at most d literals (in the usual case when $d \geq 3$), every k-DNF in $GOP(G)[X_{u,v} \leftarrow \text{Odd}(X^1_{u,v}, \ldots X^k_{u,v}), \neg X_{u,v} \leftarrow \text{Even}(X^1_{u,v}, \ldots X^k_{u,v})]$ contains at most dk variables. When such a DNF is expressed as a set of clauses using the distributive rule, the set of clauses has size at most $2^{O(dk)}$ and each clause has width at most dk. Therefore, $GOP^{\oplus k}(G)$ contains at most $O(2^{dk}n^3)$ clauses, each of width at most dk.

The graph-ordering principles are as useful starting point for proving a separation between $\text{Res}(k+1)$ and $\text{Res}(k)$ because they have polynomial size resolution refutations, but, for certain constant-degree graphs, require large width to refute in resolution.

Lemma 2 *[2] Let G be an n vertex graph. There is a resolution refutation of $GOP(G)$ of size $O(n^3)$.*

Lemma 3 *[2] There exists a constant d and a family of n vertex graphs, G_n, so that for each n, G_n has maximum degree at most d, and $w_R(GOP(G_n)) \geq n/12$.*

We build $\text{Res}(k)$ refutations for $GOP^{\oplus k}(G)$ from the small resolution refutations of $GOP(G)$.

Definition 3.3 *Let k be a positive integer and let $X_1, \ldots, X_n$ be propositional variables. Let $X_1^1, \ldots, X_1^k, X_2^1, \ldots, X_n^k$ be new variables. Let σ be the mapping given by $\sigma(X_i) = Even(X_i^1, \ldots, X_i^k)$ and $\sigma(\neg X_i) = Odd(X_i^1, \ldots, X_i^k)$. For a clause $C = \bigvee_i l_i$, let $\sigma(C) = \bigvee_i \sigma(l_i)$.*

Lemma 4 *For all k, for all clauses $A \vee X_i$ and $B \vee \neg X_i$ be clauses in the variables $X_1, \ldots, X_n$, there is a derivation of $\sigma(A) \vee \sigma(B)$ from $\{\sigma(A) \vee \sigma(X_i), \sigma(B) \vee \sigma(\neg X_i)\}$ of size $2^{O(k)}$.*

Proof: By the completeness of Res(k), there is a Res(k) refutation of the pair of k-DNFs $\{\text{Even}(X_1, \ldots, X_k), \text{Odd}(X_1, \ldots, X_k)\}$.

Because there are only k variables in the hypotheses, the size of the refutation is at most $2^{O(k)}$. Because $\sigma(X_i) = \text{Odd}(X_i^1, \ldots, X_i^k)$ and $\sigma(\neg X_i) = \text{Even}(X_i^1, \ldots, X_i^k)$, there is a derivation of $\sigma(A) \vee \sigma(B)$ from $\{\sigma(A) \vee \sigma(X_i), \sigma(B) \vee \sigma(\neg X_i)\}$ of size $2^{O(k)}$. ∎

Lemma 5 *For each k, for every graph G with n vertices and degree at most $d \geq 3$, $GOP^{\oplus k}(G)$ has a Res(k) refutation of size $2^{O(dk)} n^3$.*

Proof: With the repeated application of AND-introduction inferences, $\sigma(GOP(G))$ can be derived from $GOP^{\oplus k}(G)$ in $2^{O(dk)} n^3$ many inferences. By Lemma 2, $GOP(G)$ has a refutation of size $O(n^3)$ so by Lemma 4, $\sigma(GOP(G))$ has a Res(k) refutation of size $n^3 2^{O(k)}$. Therefore, $GOP^{\oplus k}(G)$ has a refutation of size $2^{O(dk)} n^3$. ∎

4 The Switching Lemma

The central step in the lower bound proof for Res(k) refutations of certain instances of $GOP^{\oplus(k+1)}(G)$ is an application of a random restriction which collapses k-DNFs to short decision trees.

The following distribution on restrictions will be used to prove size lower bounds for Res(k) refutations of $GOP^{\oplus(k+1)}(G)$:

Definition 4.1 *Let $k \geq 1$ be given. Let G be a graph. The distribution $\mathcal{R}_{k+1}(G)$ on partial assignments ρ to the variables of $GOP^{\oplus(k+1)}(G)$ is given by the following experiment:*

For each $(u, v) \in V(G)^2$, choose $i \in \{1, \ldots, k+1\}$ uniformly and independently. For each $j \in \{1, \ldots, k\}$, $j \neq i$, set $X_{u,v}^j$ to 0 or 1, uniformly and independently.

In order to apply the small-restriction switching lemma of Razborov, we need that the random restriction contains a completely independent random restriction as a "sub-restriction" in the following sense:

Definition 4.2 *[4] For a restriction ρ, the support of ρ, written $sup(\rho)$, is the set of variables set to 0 or 1 by ρ. For two restrictions ρ_0 and ρ, we say that ρ_0* is a sub-restriction of *ρ, written $\rho_0 \subseteq \rho$, if $sup(\rho_0) \subseteq sup(\rho)$, and ρ agrees with ρ_0 on $sup(\rho_0)$. For distributions on random restrictions, $\mathcal{R}$ and $\mathcal{R}_0$, we say that $\mathcal{R}_0$* is a sub-restriction of *$\mathcal{R}$ if there is a joint distribution $\mathcal{D}$ on pairs of assignments (ρ_0, ρ) so that:*

(1) The marginal distribution of $\mathcal{D}$ on ρ_0 is $\mathcal{R}_0$.
(2) The marginal distribution of $\mathcal{D}$ on ρ is $\mathcal{R}$.
(3) For (ρ_0, ρ) chosen according to $\mathcal{D}$, $\rho_0 \subseteq \rho$ with probability 1.

When ρ is chosen according to $\mathcal{R}_{k+1}(G)$, for each u, v the values given to $X^1_{u,v}, \ldots X^{k+1}_{u,v}$ by ρ are correlated (for example, if we know that $\rho(X^1_{u,v}) = *$ then we know that for all $i > 1$, $\rho(X^i_{u,v}) \neq *$). Therefore $\mathcal{R}_{k+1}(G)$ does *not* contain a totally independent restriction as a sub-restriction in the sense of definition 4.2. However, if we do not reveal all of $\rho \in \mathcal{R}_{k+1}(G)$, but only k variables from each group of $X^1_{u,v}, \ldots X^{k+1}_{u,v}$, then it does contain an independent sub-restriction. This is made formal in the following definition and lemma.

Definition 4.3 *Let G be a graph, and let V be a subset of the variables of $GOP^{k+1}(G)$ so that for each $(u, v) \in V(G)^2$, with $u \neq v$, exactly k of the variables $X^1_{u,v}, \ldots, X^{k+1}_{u,v}$ belong to V. Let $\mathcal{D}(V)$ be the distribution on random restrictions ρ given as follows: select κ according to $\mathcal{R}_{k+1}(G)$ and let ρ be κ restricted to the variables V. Let $\mathcal{I}(V)$ be a random restriction to these variables that with complete independence sets each variable to $*$ with probability $1/2$, and 0, 1 each with probability $1/4$.*

Lemma 6 *Let G be a graph, and let V be a subset of the variables of $GOP^{k+1}(G)$ so that for each $(u, v) \in V(G)^2$, with $u \neq v$, exactly k of the variables $X^1_{u,v}, \ldots, X^{k+1}_{u,v}$ belong to V. The restriction $\mathcal{I}(V)$ is a sub-restriction of $\mathcal{D}(V)$*

Proof: Rename the variables so that for each (u, v), $\{X^1_{u,v}, \ldots, X^k_{u,v}\} \subseteq V$. Generate a pair of restrictions (ρ_0, ρ) according to the following experiment:

(1) Choose ρ_0 according to $\mathcal{I}(V)$. Initially set $\rho = \rho_0$.
(2) For each (u, v), and for each $i = 1, \ldots k$ in turn:
   (a) If there exists $j < i$ so that $\rho(X^j_{u,v}) = *$, then, if $\rho_0(X^i_{u,v}) = *$, set $\rho(X^i_{u,v})$ to 0 or 1 (each with independent probability $1/2$), otherwise set $\rho(X^i_{u,v}) = \rho_0(X^i_{u,v})$.
   (b) If for all $j < i$, $\rho(X^j_{u,v}) \neq *$, then if $\rho_0(X^i_{u,v}) \neq *$, set $\rho(X^i_{u,v}) = \rho_0(X^i_{u,v})$, otherwise set $\rho(X^i_{u,v}) = *$ with probability $\frac{1}{k+2-i}$, and 0,1

each with probability $\frac{1}{2}\left(1-\frac{1}{k+2-i}\right)$.

Clearly the experiment produces ρ_0 according to the distribution $\mathcal{I}(V)$ and ρ so that $\rho_0 \subseteq \rho$. We now show that ρ is generated according to the distribution $\mathcal{D}(V)$. First of all, for any $X^i_{u,v}$ with $\rho(X^i_{u,v}) \neq *$, the 0/1 value of $\rho(X^i_{u,v})$ is chosen uniformly from $\{0,1\}$ completely independent of the values received by the other variables. Next, it is clear that for any ordered pair (u,v) there is always at most one $i \in [k]$ with $\rho(X^i_{u,v}) = *$.

Finally, we show by induction on $i \in [k]$ that for each (u,v), $Pr[\rho(X^i_{u,v}) = *] = \frac{1}{k+1}$. Fix a pair of vertices (u,v). First note that by the definition of the experiment, $Pr[\rho(X^i_{u,v}) = * \mid \forall j < i,\ \rho(X^j_{u,v}) \neq *] = \frac{1}{k+2-i}$. For each i, $1 \leq i \leq k+1$, let B_i denote the event $\forall j < i$, $\rho(X^j_{u,v}) \neq *$. In the base case: $Pr[\rho(X^1_{u,v}) = *] = \frac{1}{k+1}$. For the induction step:

$$\begin{aligned} Pr[\rho(X^i_{u,v}) = *] = &\quad Pr[\rho(X^i_{u,v}) = * \mid B_i] \cdot \textstyle\prod_{j<i} Pr[\rho(X^j_{u,v}) \neq * \mid B_j] \\ = &\ \tfrac{1}{k+2-i} \cdot \textstyle\prod_{j<i}\left(1-\frac{1}{k+2-j}\right) = \frac{1}{k+2-i} \cdot \prod_{j<i}\left(\frac{k+1-j}{k+2-j}\right) = \frac{1}{k+1} \end{aligned}$$

■

Definition 4.4 *A DNF is said to be* pseudomonotone *if every variable in the DNF appears only positively or only negatively.*

Definition 4.5 *Let F be a k-DNF in the variables of $GOP^{\oplus(k+1)}(G)$. We say that F is* amenable *if F is pseudo-monotone and for each $u, v \in V(G)$, $u \neq v$, at most k variables of $X^1_{u,v}, \ldots, X^{k+1}_{u,v}$ appear in F.*

Lemma 7 *(claim (13) in the proof of Lemma 4.4 of [4]) There exists a constant $\epsilon_0 > 0$ so that for any amenable k-DNF F,*

$$Pr_{\rho_0 \in \mathcal{I}(Vars(F))}[H(F\restriction_\rho) > h] \leq e^{-h(\epsilon_0/2)^{2k}}$$

By Lemma 6, for any amenable k-DNF F, $\mathcal{I}(Vars(F))$ is a subrestriction of $\mathcal{R}_{k+1}(G)$ on the variables of $Vars(F)$. Therefore, a random restriction from $\mathcal{R}_{k+1}(G)$ also collapses an amenable DNF.

Corollary 8 *There exists a constant $\epsilon_0 > 0$ so that for any amenable k-DNF F,*

$$Pr_{\rho \in \mathcal{R}_{k+1}(G)}[H(F\restriction_\rho) > h] \leq e^{-h(\epsilon_0/2)^{2k}}$$

Lemma 9 *[4] Let $\epsilon, \delta > 0$ be given, let F be a k-DNF, let $\mathcal{R}$ be a distribution on partial assignments to the variables, and let $\mathcal{G}_F$ be a distribution on sub-*

DNFs of F so that for every term $t \in F$, $Pr_{F_0 \in \mathcal{G}_F}[t \in G] \geq \epsilon$ and for every F_0 in the support of $\mathcal{G}$, $Pr_{\rho \in \mathcal{R}}[H(F_0 \restriction_\rho) > h] \leq \delta$. The following inequality holds:

$$Pr_{\rho \in \mathcal{R}}[H(F \restriction_\rho) > h(\frac{2k}{\epsilon} + 1)] \leq 2\delta/\epsilon$$

Definition 4.6 *Fix a DNF F in the variables of $GOP^{\oplus(k+1)}(G)$. Let $\mathcal{G}_F$ be the distribution on sub-DNFs F_0 of F that arises as follows: choose a restriction ρ according to $\mathcal{R}_{k+1}(G)$, and let $F_0 = \{t \in F \mid t \restriction_\rho = 1\}$.*

Note that every DNF F_0 in the support of $\mathcal{G}_{k+1}(F)$ is amenable.

Lemma 10 *Fix a k-DNF F in the variables of $GOP^{\oplus(k+1)}(G)$, and let $t \in F$ be given.*

$$Pr_{F_0 \in \mathcal{G}_F}[t \in F_0] \geq 1/4^k$$

Proof: By definition the probability that $t \in F_0$ is the probability that t is satisfied by $\rho \in \mathcal{R}_{k+1}(G)$. Consider setting each variable of t in turn. The probability that a variable is set to 0 or 1 is always $\geq 1/(k+1-(k-1)) = 1/2$. Therefore, the probability that every variable is set is at least $1/2^k$. Conditioned on this event, the term is satisfied with probability at least $1/2^k$. ∎

Lemma 11 *Let F be a k-DNF in the variables $GOP^{\oplus(k+1)}(G)$.*

$$Pr_{\rho \in \mathcal{R}_{k+1}(G)}[H(F \restriction_\rho) > h(k \cdot 2^{2k+1} + 1)] \leq 2^{2k+1} \cdot e^{-h(\epsilon_0/2)^{2k}}$$

Proof: By Lemma 10, the distribution $\mathcal{G}_F$ is a fractional cover of F such that when F_0 is selected according to $\mathcal{G}_F$, each term of F appears in F_0 with probability at least $1/4^k$. The DNF F_0 is amenable with probability 1, and by corollary 8, $Pr_{\rho \in \mathcal{R}_{k+1}}(G)[H(F_0 \restriction_\rho) > h] \leq e^{-h(\epsilon_0/2)^{2k}}$. Therefore, by Lemma 9,

$$Pr_{\rho \in \mathcal{R}_{k+1}(G)}[H(F \restriction_\rho) > h(k \cdot 2^{2k+1} + 1)] = Pr_{\rho \in \mathcal{R}_{k+1}(G)}[H(F \restriction_\rho) > h(\frac{2k}{4^{-k}} + 1)]$$

$$\leq \frac{2}{4^{-k}} \cdot e^{-h(\epsilon_0/2)^{2k}} = 2^{2k+1} \cdot e^{-h(\epsilon_0/2)^{2k}}$$

∎

5 Separation Between Res(k) and Res($k+1$)

Theorem 12 *There exist constants $\beta, \gamma, d > 0$ and a family of graphs G on n vertices with maximum degree d so that whenever $k = k(n) \leq \beta \log n$, Res($k$) refutations of $GOP^{\oplus(k+1)}(G)$ require size at least 2^{n^γ}.*

By Lemma 3 we may choose a positive integer d and a family n vertex graphs of maximum degree at most d so that $w_R(GOP(G_n)) \geq n/12$. Let k and n be given. Let $G = G_n$. By Lemma 11 we have that for every k-DNF F

$$\Pr_{\rho \in \mathcal{R}_{k+1}(G)} [H(F \restriction_\rho) > (n/12 - 1)/k] \leq 2^{2k+1} \cdot e^{-\left(\frac{k \cdot 2^{2k+1}+1}{k}\right)(n/12-1)(\epsilon_0/2)^{2k}}$$

Choose $\beta, \gamma > 0$ so that when $k \leq \beta \log n$, $\Pr_{\rho \in \mathcal{D}} [h(F \restriction_\rho) > (n/12 - 1)/k] < 2^{-n^\gamma}$. Suppose for the sake of contradiction that Γ is a Res(k) refutation of $GOP^{\oplus(k+1)}(G)$ of size less than 2^{n^γ}. By the union bound, with probability > 0, every line F of Γ has $H(F \restriction_\rho) \leq (n/12 - 1)/k$. By Theorem 1, $GOP^{k+1}(G) \restriction_\rho$ has a resolution refutation of width at most $n/12 - 1$. Note that $GOP^{\oplus(k+1)}(G) \restriction_\rho$ is an instance of $GOP(G)$, possibly with some of the edge variables inverted. However, inverting some variables does not affect the width required for a resolution refutation, so $GOP(G)^{\oplus(k+1)} \restriction_\rho$ requires width at least $n/12$ to refute in resolution, contradiction.

Acknowledgment: The author would like to thank Alexander Razborov for encouraging the write-up of this note.

References

[1] A. Atserias, M. Bonet, On the automatizability of resolution and related propositional proof systems, Information and Computation 189 (2) (2004) 182–201.

[2] N. Segerlind, S. Buss, R. Impagliazzo, A switching lemma for small restrictions and lower bounds for k-DNF resolution, SIAM Journal on Computing 33 (5) (2004) 1171–1200, preliminary version appeared in FOCS 2002.

[3] J. Håstad, Almost optimal lower bounds for small depth circuits, in: Advances in Computing Research, Vol. 5, JAI Press, 1989, pp. 143–170.

[4] A. Razborov, Pseudorandom generators hard for k-DNF resolution and polynomial calculus resolution, submitted. Available at `http://genesis.mi.ras.ru/~razborov/` (2003).

[5] A. Goerdt, Unrestricted resolution versus N-resolution, Theoretical Computer Science 93 (1) (1992) 159–167.

[6] M. Bonet, N. Galesi, A study of proof search algorithms for resolution and polynomial calculus, in: Proceedings of the Fortieth Annual IEEE Symposium on Foundations of Computer Science, 1999, pp. 422–431.